Lab 10.9.1 Configure a Catalyst 6000 IDSM

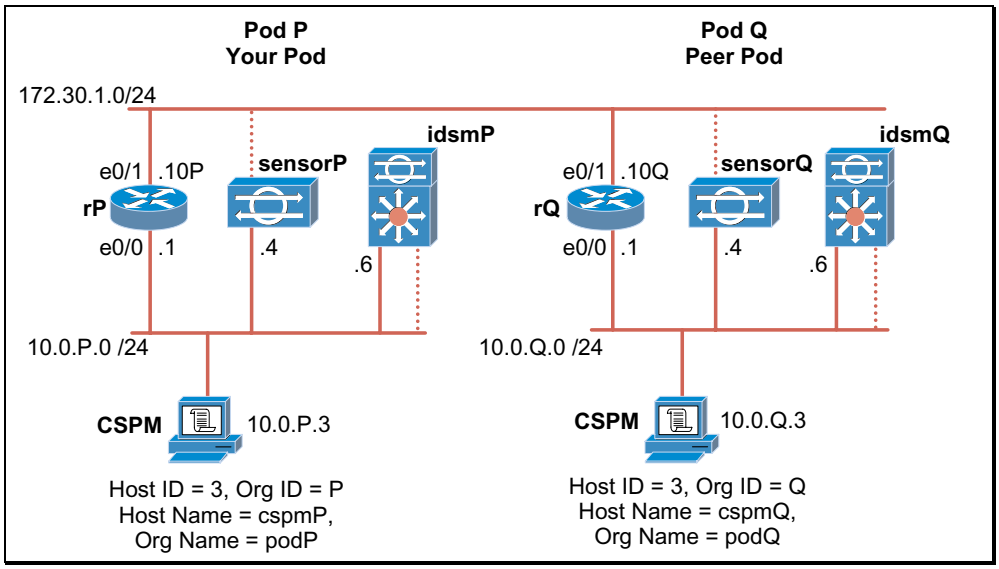
Objective

In this lab exercise you will complete the following tasks:

- Initialize the Catalyst 6000 IDSM.
- Configure the Catalyst 6000 Family switch to capture traffic for Intrusion Detection analysis.
- Add the IDSM to an existing network topology in CSPM.
- Apply a signature update to the IDSM application partition.
- Transfer the IDSM System Status report to your CSPM host.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



Setup

Before starting this lab exercise, set up your equipment so that you can ensure you have connectivity to the switch that you are going to configure. Verify that your pod has an FTP server with a public directory with write privileges for file transfers.

Directions

Your task in this lab exercise is to configure the Catalyst 6000 Family switch and IDSM to detect alarms and send alarm notifications to CSPM. Then you will add the IDSM to an existing CSPM network topology. Follow the convention where **P**=pod number and **PVLAN**=300 + **P**. For example, student pod 3 would have **PVLAN**= 303. Your instructor will assign your Module number, **M**, and the IP address of the switch, **SW**.

Your instructor will provide you with the values to complete the following table.

Parameter	Value
PVLAN	
M	
SW	

Task 1—Initialize the IDSM

Perform the following lab steps to initialize the IDSM.

Step 1 From your Windows host, telnet to the switch.

```
c:> telnet SW
```

(where SW = IP address of switch)

Step 2 Disable console error messages during your telnet session into the switch.

```
switch> (enable) set logging session disable
```

Step 3 Session and log into your idsm:

```
switch> session M
```
(where M = module number assigned)

```
login: ciscoids
password: attack
```

Step 4 Run the **setup** command:

```
# setup
```

Step 5 Follow the system configuration dialog and enter the following CIDS Communications Infrastructure parameters:

Parameter	Value
IDSM virtual terminal password	Keep the default setting of *current*
Sensor's IP address	**10.0.P.6** (where *P* = pod number)
Sensor's IP subnet mask	**255.255.255.0**
Sensor's default gateway	**10.0.P.1** (where *P* = pod number)
Sensor's host name	**idsmP** (where *P* = pod number)
Sensor's host id	**6**
Sensor's host post office port	**45000**
Sensor's organization name	**podP** (where *P* = pod number)
Sensor's organization id	**P** (where *P* = pod number)
Director's IP address	**10.0.P.3** (where *P* = pod number)
Director's host name	**directorP** (where *P* = pod number)
Director's host post office port	Keep the default setting of *45000*
Director's host id	**3**

 Copyright © 2001, Cisco Systems, Inc.

Parameter	Value
Director's heart beat interval	Keep the default setting of *5*
Director's organization name	**podP** (where *P* = pod number)
Director's organization id	**P** (where *P* = pod number)

Note The IDSM command and control port is assigned the Sensor's settings.

Step 6 After entering and reviewing all communication parameters enter **yes** when prompted to apply this configuration. If you made any mistakes, enter **no** and re-run the **setup** command.

Note The IDSM will reset after you accept and apply the configuration. You will be logged out and returned to the switch prompt.

Task 2—Configure the switch for ID analysis

Perform the following lab steps to configure the switch for Intrusion Detection analysis using the VLAN ACL (VACL) feature. Follow the convention where **P**=pod number and **PVLAN**=300 + **P**. For example, student pod 3 would have **PVLAN**= 303. Your instructor will assign your Module number, **M**.

Step 1 Go into privileged mode:

```
switch> enable
Password: cisco
switch>(enable)
```

Step 2 Verify your IDS module status is **ok**. Do *NOT* continue until the module status is ok.

```
switch>(enable) show module M
switch> (enable) show module 3
Mod Slot Ports Module-Type              Model              Sub Status
3   3    2     Intrusion Detection System WS-X6381-IDS       no  ok
```

Step 3 Set the command and control port to the VLAN that can communicate with CSPM:

```
switch>(enable) set vlan PVLAN M/2
```

(where *PVLAN* = 300 + pod number, and M=module number assigned)

Note You will receive an error if you attempt to add the command and control interface to a VLAN if the module status is not *ok*.

Step 4 Create the VACL to capture all IP traffic destined to your VLAN:

```
switch#(enable) set security acl ip SPAN_PVLAN permit ip any any capture
```

(where PVLAN = 300 + pod number)

Step 5 Commit the VACL to NVRAM:

```
switch#(enable) commit security acl SPAN_PVLAN
```

(where PVLAN = 300 + pod number)

Step 6 Map the VACL to the VLAN:

```
switch#(enable) set security acl map SPAN_PVLAN PVLAN
```

(where PVLAN = 300 + pod number)

Note The destination capture port is assigned by default to *IDSM Port 1*.

Task 3—Verify the switch and IDSM Configuration

Perform the following lab steps to verify the switch and IDSM configurations are correct.

Step 1 Display your switch's IDSM configuration:

```
switch>(enable) show config M
(where M = module number assigned)
switch> (enable) show conf 3
This command shows non-default configurations only.
Use 'show config <mod> all' to show both default and non-default configurations.
..............
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!#time: Sat Nov 25 2000, 02:55:48
!
# default port status is enable
!
!
#module 3 : 2-port Intrusion Detection System
set port gvrp     3/2  disable
set security acl capture-ports 3/1
end
```

Step 2 Display the switch's security ACL settings:

```
switch>(enable)show security acl
ACL                                 Type VLANS
-------------------------------  ---- -----
SPAN_301                          IP   301
switch>(enable)show security acl map PVLAN
(where PVLAN = 300 + pod number)
switch>(enable)show security acl map 301
VLAN 301 is mapped to IP ACL SPAN_301.
```

Step 3 Session into your IDS module and display the IDSM configuration:

```
idsm# show configuration
Using 46178304 out of 267702272 bytes of available memory
!
Using 460935168 out of 4211310592 bytes of available disk space
!
```

 Copyright © 2001, Cisco Systems, Inc.

```
Sensor version is : 2.5(1)S1
!
Sensor application status:
nr.postofficed       running
nr.fileXferd         running
nr.loggerd           running
nr.packetd           running
nr.sapd              running
Configuration last modified Tue Nov 07 01:03:54 2000
Sensor:
IP Address:                 10.0.0.6
Netmask:                    255.255.255.0
Default Gateway:            10.0.0.1
Host Name:                  idsm0
Host ID:                    6
Host Port:                  45000
Organization Name:          pod0
Organization ID:            100
Director:
IP Address:                 10.0.0.84
Host Name:                  director84
Host ID:                    84
Host Port:                  45000
Heart Beat Interval (secs): 5
Organization Name:          pod0
Organization ID:            100on
```

Step 4 Display the IDSM logfile:

```
idsm# diag
idsm#(diag) show eventfile current
4,0,2000/11/25,01:07:12,2000/11/25,01:07:12,10000,6,100,OUT,OUT,5,997,0,TCP/IP,0.0
.0.0,0.0.0.0,0,0,0.0.0.0,84.100 route 1 down
4,1,2000/11/25,01:07:29,2000/11/25,01:07:29,10000,6,100,OUT,OUT,1,0,0,TCP/IP,0.0.0
.0,0.0.0.0,0,0,0.0.0.0,postofficed initial notification msg
```

Task 4—Add the IDSM to CSPM

Perform the following lab steps to add the IDSM to an existing network topology in CSPM:

Step 1 From your Windows host, launch the CSPM software. Choose **Start>Programs>Cisco Systems>Cisco Secure Policy Manager>Cisco Secure Policy Manager** from the menu bar.

Step 2 Log into the CSPM database as *Administrator* with the password *attack*.

Step 3 Choose the **Add Sensor** wizard from the CSPM menu bar. The Sensor Identification window opens.

Step 4 Enter the Sensor Identification parameters.

Parameter	Value
Sensor's host name	**idsmP** (where *P* = pod number)

Sensor's host id	**6**
Sensor's organization id	**P** (where *P* = pod number)
Sensor's organization name	**podP** (where *P* = pod number)
Sensor's IP address	**10.0.P.6** (where *P* = pod number)
Policy Enforcement Associated Network Service	Keep the default setting of *Cisco Post Office*

Step 5 Click **Next** to continue. The Sensor Configuration window opens.

Step 6 Choose the **Sensor Version** and **Signature Template** to apply to the IDSM.

Your instructor will provide you with the values to complete the following table.

Parameter	Value
Sensor version	
Signature template	

Step 7 Click **Next** to continue. The Ready to Proceed window opens.

Step 8 Verify the PostOffice parameters. Click **Finish** to add the IDSM to the network topology.

Step 9 Click **Update** on the toolbar to save your changes and update the configuration files.

Step 10 Select **idsmP** (where *P* = pod number) from the Network Topology Tree.

Step 11 Select the **Command** tab in the Sensor view panel.

Step 12 Click the **Approve Now** button in the Command Approval section. Wait for the configuration files to be downloaded to the Sensor.

Step 13 After you get an Upload completed message in the Status section proceed to the next task.

Note Notify the instructor that you have completed these tasks before proceeding.

Task 5—Apply a Signature Update

Perform the following lab steps to apply a signature update to the IDSM application partition:

Step 1 Telnet into the switch from your Windows host.

Step 2 Session into your IDSM.

```
switch> session M
```
(where M = module number assigned)

```
login: ciscoids
Password: attack
```

Step 3 Go into configuration mode.

```
idsm# config t
```

 Copyright © 2001, Cisco Systems, Inc.

Step 4 Apply the signature update.

Your instructor will provide you with the values to complete the following table.

Parameter	Value
FTPSITE	
USERNAME	
FTPDIR	
FILENAME	

```
idsm#(config) apply signatureupdate site FTPSITE user USERNAME dir FTPDIR file
FILENAME
```

Step 5 A warning message is displayed. Enter **yes** when prompted to continue with the install.

Step 6 Enter the password **attack** when prompted. Wait for the file to download. When the download is completed, the IDSM will shutdown and restart. You will be logged out and returned to the switch prompt.

Step 7 Session into your IDSM once the module status is **ok**.

Step 8 Verify the service pack was installed.

```
idsm# show config
```

Task 6—Transfer the IDSM System Status Report

Perform the following lab steps to transfer the IDSM system status file:

Step 1 Telnet into the switch from your Windows host.

Step 2 Session into your IDSM.

```
switch> session M
```
(where M=module number assigned)

```
login: ciscoids
Password: attack
```

Step 3 Go into diagnostics mode.

```
idsm# diag
```

Step 4 Transfer the system status file to your FTP server.

```
idsm(diag)# report systemstatus site 10.0.P.3 user ftp dir .
```

(where P=pod number)

Step 5 Enter **yes** when prompted to continue generating the system status report.

Step 6 Enter the password **attack** when prompted.

Step 7 Launch your web browser from your windows host.

Step 8 Open the IDSM system status report. In your web browser, choose **File>Open**. Locate the file in your FTP directory. Use your browser's browse feature.

```
C:\InetPub\ftproot\idsm0SystemStatusReport.html
```

Completion Criteria

You completed this lab exercise if you were able to do the following:

- Successfully configure the IDSM to communicate with CSPM.
- Successfully configure the switch to capture traffic.
- Successfully add the IDSM to an existing network topology in CSPM.
- Successfully apply the signature update to the IDSM application partition.
- Successfully transfer the IDSM System Status report to the CSPM host.

 Copyright © 2001, Cisco Systems, Inc.